REMARKS

The above amendments to the above-captioned application along with the following remarks are being submitted as a full and complete response to the Office Action dated September 9, 2005. In view of the above amendments and the following remarks, the Examiner is respectfully requested to give due reconsideration to this application, to indicate the allowability of the claims, and to pass this case to issue.

Status of the Claims

As outlined above, claims 13 - 21 are currently pending in this application, wherein claims 13, 16 and 19 are being amended to more particularly point out and distinctly claim the subject invention. Support for the recitation of the claims and claim amendments outlined above may be found throughout the specification as will be discussed further hereinbelow. Applicant hereby submits that no new matter is being introduced into the application through the submission of this supplemental response.

Prior Art Rejections

The Examiner rejected claims 13-21 under 35 U.S.C. § 102(e) as being anticipated by Hohle (U.S. Patent No. 6,199,762). Applicants have reviewed the above-noted rejection and hereby respectfully traverse.

The present invention as set forth in claim 13 is directed to a smart card system, comprising: a smart card issuance/management system configured to perform issuance and management of a smart card; and a smart card service providing/managing system configured to perform issuance and management of an application loaded on the smart card, wherein the smart card issuance/management system and the smart card service providing/managing system are operatively connected to each other through a network such that information exchange is achieved by transmitting and receiving electronic messages through the network. Each of the electronic messages, which is exchanged between the smart card issuance/management system and smart card service providing/managing system, is uniquely identified using a message ID. Data of the smart card issuance/management system and the smart card service providing/managing system is stored using the message ID as a key. In addition, the information exchange between the smart card issuance/management system and the smart card service providing/managing system includes at the time of initial issuance of the smart card, the smart card issuance/management system sending an application loading permission which permits the smart card service providing/management system to load an application into the smart card, at the time of the initial issuance of the smart card, the smart card service providing/managing system sends the application loading permission and the application and loads the application in the smart card, and at the time of the reissuance of the smart card, the smart card service providing/managing system receive the card attribute data, which can be identified only by the card issuer, from the smart card, sends the card attribute information and an application ID of the application to the smart card issuance/management system, the smart card issuance/management system searches the message ID of the application loading permission which was used when the smart the card issuance/management system sent the application loading permission for loading the application to the smart card using the sent card attribute information, which identifies the smart card service providing/managing system searches an examination result of permission for loading the application at the time of initial loading application using the message ID as the key.

According to claim 16, the present invention is directed to a smart card issuance/management system configured to perform issuance and management of a smart card and configured to connect to a smart card service providing/managing system through a network, wherein information exchange is achieved by transmitting and receiving electronic messages through the network. Each of the electronic messages, which are exchanged between the smart card issuance/management system and smart card service providing/managing system, is uniquely identified using a message ID. Data of the smart card issuance/management system and the smart card service providing/managing system is stored using the message ID as a key. At the time of initial issuance of the smart card, the smart card issuance/management system sends an application loading permission which permits the smart card service providing/management system to load an application into the smart card; and at the time of initial issuance of the smart card, the smart card issuance/management system searches a message ID which was used when the smart card issuance/management system sent the application loading permission for loading the application to the smart card of the application loading permission using card attribute data, which identifies the smart card and can be identified only by the card issuer, as a key, and sends the message ID of the application loading permission using card attribute data, which was used when the smart card issuance/management system sent the application loading permission for loading the application to the smart card.

Further, according to claim 19, the present invention is directed to a smart card service providing/managing system configured to perform issuance and management of a smart card and 'configured to connected to an IC card service issuance/management system configured to performed issuance and management an application loaded on the smart card, through the network, wherein information exchange is achieved by transmitting and receiving electronic message through the network. Each of the electric messages, which is exchanged between the smart card issuance/management system and smart card service providing/managing system, is uniquely identified using a message ID. The data of the smart card issuance/management system and the smart card service providing/managing system is stored using the message ID as a key. At the time of initial issuance of the smart card, the smart card service providing/managing system receives an application loading permission from the smart card issuance/management system, which permits the smart card service providing/management system to load an application into the smart card, and loads the application to the smart card; and at the time of reissuance of the smart card, the service providing/managing system receives the card attribute data, which can be identified only by the card issuer, from the smart card which identified the smart card, sends the card attribute data and an application ID of the application, receives the message ID of the application loading permission, which was used when the smart card issuance/management system sent the application loading permission. for loading the application to the smart card, and searches an examination result of permission for loading the application at the time of initial loading application using the message ID as the key.

The present claimed invention relates to a smart card system having a policy that prohibits notification of card attribute data to outside. One of main features of the present claimed invention is that when loading an application into a reissued card is required, a message ID, which is used when permission for loading has been exchanged between the card issuer and the service provider and uniquely identifies an electronic message exchanged with a service provider, is searched and by using this message ID, information related to application loading, which is used the application has been loaded in the old smart card, can be read (see page 11, line 7 to page 13, line 10 and page 33, line 11 to page 36, line 4).

As outlined in the claim amendments set forth above, Applicants would like to clarify the following aspects of the present invention:

(1) The "electronic message" is exchanged between the smart card issuance/management system and smart card service providing/managing system;

(2) The smart card issuance/management system sends an application loading permission which permits the smart card service providing/management system to load an application into the smart card;

(3) The "card attribute data" can be identified only by the card issuer;

(4) The "message ID" is used when the smart card issuance/management system sends the application loading permission for loading the application to the smart card; and

(5) An examination result is for permission for loading the application.

Since all the responsibilities on an IC card belong to a card issuer, it is not permissible in general for a service provider to freely load an application through a terminal. In view of this fact, the service provider requests permission for loading an application to the card issuer. The card issuer then checks if the requested application is invalid or not and the service provider requesting an application is invalid or not, and then the card issuer issues a loading permission for loading the application. The service provider transmits both the accepted the loading permission for loading application and the application to an IC card to realize loading of the application (see page 3, line 2 from the bottom to page 5, line 3).

When the IC card must be reissued, a card user goes again to each of the service providers and files a request for re-loading the application already stored in the old card. In this case, since the most important feature of the IC card is to achieve a high degree of safety and security, 'the service provider cannot employ such a simple method as one for trusting the filing of re-loading performed by the user (see page 6, line 6 to page 7, line 16). Accordingly, a procedure for filing for allowing issuance from the service provider to the card issuer must be taken again and the burden is imposed on both the user and service provider (see page 6, line 6 to page 7, line 5).

The above-described circumstances would be a problem if it assumed that the card issuer does not inform outside parties (i.e., service providers) of any attributive data such as a card ID in order to protect their security/privacy. That is, the service provider cannot extract any related information such as a card number from the IC card. The service provider can extract only information on card attributes made in such a format that only the card issuer can identify it by use of a method of encrypting the card ID with a public key of the card issuer and the like (see page 12, last line to page 13, line 10).

The present invention resolves the problem described above wherein, when re-loading of the application into the IC card is requested by the card user, the service provider extracts the card attribute data in such a manner as to be capable of being identified by the card issuer only from the IC card, and makes an inquiry to the card issuer together with "the application ID" desired to be stored. Then, the card issuer retrieves with a key of the card attribute data by decoding the card attribute data with own secret key. More specifically, the card issuer collates "whether or not the IC card requested for inquiry is a re-issue card", and collates "a message ID used when the loading permission of loading the application requested for re-loading into the old card is exchanged", and then transmits the result of inquiry to the service provider. "The message ID" defined herein is an ID for uniquely identifying an electronic message when the electronic message is exchanged between the card issuer and the service provider.

The service provider can acknowledge, through this series of procedures, whether or not the IC card submitted by the user is the re-issue card. Further, the service provider can confirm that the application requested by the user for its re-loading has also been stored in the old card by collating an IC card application data base with a message ID of the electronic message used when the loading permission for loading into the old card is exchanged applied as a key. Further, it becomes possible to make an inquiry for the information required for re-loading the application such as a result of examination at the time of loading it and the like and to judge whether or not the re-loading can be carried out (see page 33, line 11 to page 36, line 23).

As described above, both the card issuer and the user are not required to reveal the card attribute data such as the card ID (including private information or the like) when the service provider collates information requisite for re-loading of the application by using, not the card attribute data, but instead the message ID applied as a key, and thus security can be maintained in that the attributive data such as the card ID that may become private information is not revealed. Further, the service provider can re-load the application without obtaining any permission from the card issuer again. Even more, it becomes possible to reduce the burden on the user and the service provider when the application is re-loaded (see page 11, line 7 to page 11, line 15 and page 33, line 11 to page 36, line 23).

In the Office Action, the Examiner asserts that the message ID of the present invention corresponds to the initialization data (e.g., account number, serial number, default preferences, and the like) of Hohle '762. However, Applicants will point out that the information referred to as the initialization data in Hohle '762 is in fact "the card attribute data" in the specification of the present invention, and the initialization data is information that is quite different in meaning from "the message ID" of the present invention. The message ID as described in the specification of the present invention means a combination of business person identification information of the card issuer, business person identification information of the service provider, and a message sequence number, for example, and the message ID is information for uniquely discriminating the electronic message between the card issuer and the service provider (see page 11, line 16 to page 12, line 25; original claim 14).

In addition, the attribute data is information that is not absolutely acknowledged by the service provider in view of the security privacy as described above. Accordingly, in the present invention, only the card attribute data is exchanged between the card issuer and the service provider in such a manner that only the card issuer can acknowledge it. Hohle '762 fails to disclose and suggest that attribute data is outputted in a format identifiable by the card issuer only from the IC card (see page 36, line 24 to page 37, line 2; steps 804 and 805 in Figure 8).

In particular, Hohle '762 does not disclose and suggest how to address the restrictive conditions described above nor how to resolve such conditions in order to maintain the security intended and achieved by the present invention wherein attributive information, such as card ID, is not revealed to outside parties (i.e., service providers).

Moreover, Hohle '762 fails disclose any step or operation wherein "attribute data is outputted in a format identifiable by the card issuer only from the IC card (see page 36, line 24 to page 37, line 2; steps 804 and 805 in Figure 8). Therefore, Hohle '762 cannot also disclose or suggest any subsequent procedure of using the message ID (steps 806, 807 in Figure 8). Because of these shortcomings, Hohle '762 cannot disclose or suggest any method or system for reducing the burden imposed on both the user and service provider when an application is to be re-installed as does the present invention. Rather, the present invention as a whole is distinguishable and thereby allowable over the cited prior art references.

Conclusion

In view of all the above, Applicant respectfully submits that certain clear and distinct differences as discussed exist between the present invention as now claimed and the prior art upon which the rejection in the Office Action relies. These differences are more than sufficient that the present invention as now claimed would not have been anticipated nor rendered obvious given the prior art. Rather, the present invention as a whole is distinguishable, and thereby allowable over the prior art.

Favorable reconsideration of this application as amended is respectfully solicited. Should there be any outstanding issues requiring discussion that would further the prosecution and allowance of the above-captioned application, the Examiner is invited to contact the Applicant's undersigned representative at the address and phone number indicated below.

Respectfully submitted,

Stanley P. Fisher
Registration Number 24,344

Juan Carlos A. Marquez
Registration Number 34,072

REED SMITH LLP
3110 Fairview Park Drive
Suite 1400
Falls Church, Virginia 22042
(703) 641-4200

January 9, 2006
SPF/JCM